USER AUTHENTICATION METHOD, AND STORAGE MEDIUM, APPARATUS AND SYSTEM THEREFOR

Abstract

The invention provides a user authentication method and apparatus whereby, even when multiple verifiers correspond with a prover, safe user authentication is ensured while zero knowledge property is acquired. In an example embodiment, at step 1, a prover calculates A = F(g, a) using a random number a, and transmits A to a verifier (process Ps1, communication T1). At step 2, the verifier uses a random number b to calculate cryptograms B = F(g, b) and X = F(A, b), and transmits B and X to the prover (process Qs1, communication T2). At step 3, the prover determines whether X = F(B, a) has been established. If X = F(B, a) has not been established, the prover halts performance of the protocol procedures. If X = F(B, a) has been established, the prover 10 uses a random number c to calculate C = F(g, c) and Y = F(B, c) and thereafter calculates Z = H(a, Y, s), and then transmits C, Y and Z to the verifier 40 (process Ps2, communication T3). At step 4, the verifier determines whether Y = F(C, b) and A = J(v, Y, g, Z) have been established. If Y = F(C, b) and A = J(v, Y, g, Z) have been established, the verifier 40 accepts the identity of the prover 10. If Y = F(C, b) and A = J(v, Y, g, Z) have not been established, the verifier rejects the identity of the prover (process Qs2).